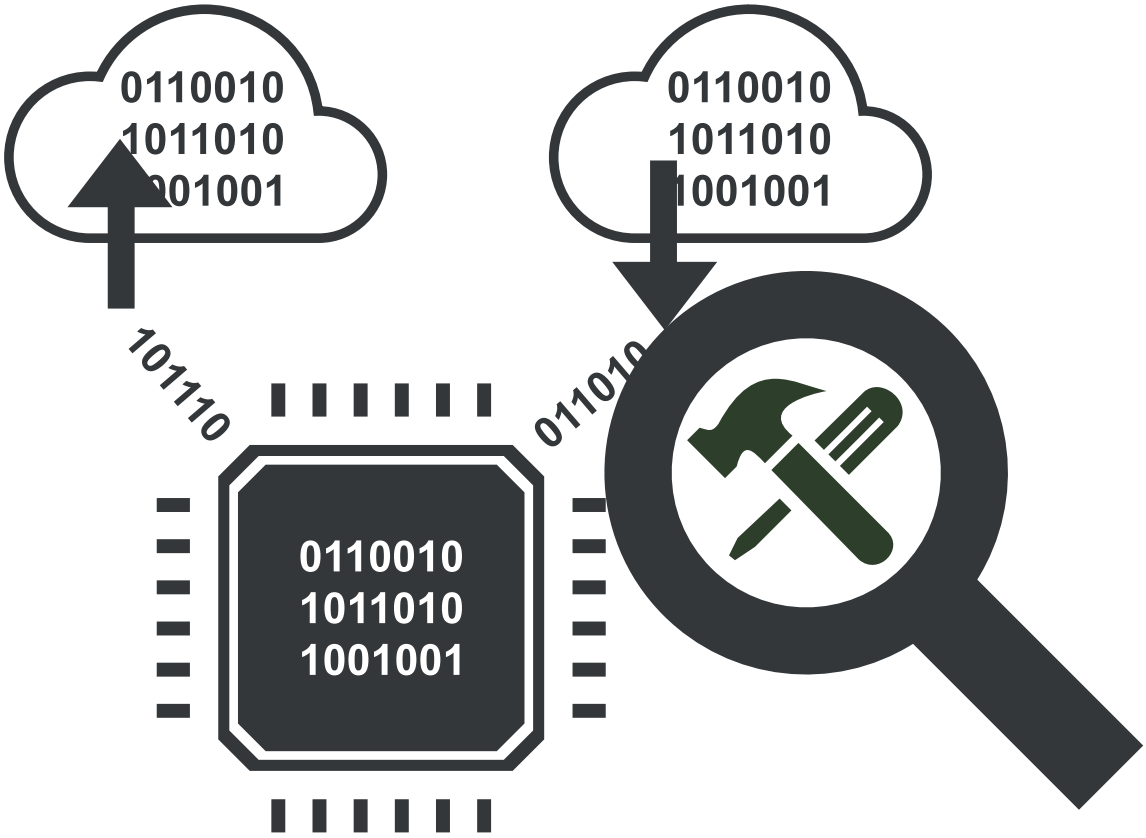

5 häufige Fehler vermeiden

Die digitale Epoche

Mit den digitalen Möglichkeiten steigen die administrativen Aufgaben.

Inhaltsverzeichnis

Impressum:

Herausgeber:
Datenschutz | Einfach | Digital | Gestalten
eine Initiative der
Marc Weber Management GmbH

Autor:
Marc Weber

Bezugsquelle:
Marc Weber Management GmbH
Lackerbauerstraße 23
81241 München
www.dedg.de
dedg@marcweber.de
Telefon 089 66 62 86 0
Fax 089 66 62 86 25

Stand:
März 2018

Bildnachweis:
Marc Weber Management GmbH

Vorwort

Mit der dritten Ausgabe beleuchten wir nun auch Themen rund um die Digitalisierung und den neuen Technologien. Cloud, Disruption, Big Data, ja sogar Industrie 4.0 machen mittlerweile auch nicht mehr vor kleinen und mittleren Unternehmen halt. Zahlreiche Prozesse, seien es nun administrative Verwaltungsangelegenheiten oder auf die Kundschaft ausgerichtete Angebote, geraten in den digitalen Fokus. Neue Anwendungen und Applikationen versprechen nur allzu gern mehr Effizienz und weniger Kosten bis hin zu Personaleinsparungen. Der Mehraufwand im Bereich Datenschutz wird dabei gerne klein gehalten oder erst gar nicht erwähnt. Eine schwierige Herausforderung für Unternehmen, die nun auch Fachpersonal für den Bereich Datenschutz benötigen.

Ihr Marc Weber

1. Die Wahl des Cloud Anbieters

Die Lage

Die Auslagerung an Daten in die Cloud ist insbesonders für kleinere Unternehmen eine lukrative Errungenschaft der digitalen Welt. Inhaber kleinerer Betriebe können so auf die Daten nicht nur im Betrieb selbst, sondern auch beispielsweise von Zuhause aus zugreifen, ohne dabei lästige Hardware mit sich herumschleppen zu müssen. Aber auch größeren Unternehmen mit Niederlassungen bietet der Onlinespeicher die Möglichkeit, die Datenbestände zentral zu halten. Mit den online verfügbaren Daten können auch die Außendienstmitarbeiter in das Datennetz eingebunden werden um über Anwendungen auf dem Smartphone die nötigen Daten in Echtzeit abfragen zu können.
Jedoch birgt die Cloud für personenbezogene Daten auch datenschutzrechtliche Sackgassen. Zumeist werden Dienstleister anhand des Preises und nicht nach der Zuverlässigkeit ausgewählt. Dabei findet der konkrete Serverstandort wie auch die Prüfung des Sicherheitskonzeptes des Dienstleisters kaum Beachtung. Schnell können sich sicherheitskritische Situationen und unerlaubte Datenübermittlungen ergeben.

Der Ansatz

Die Wahl eines Cloudanbieters sollte aus den Erwägungen des Datenschutzes und der Datensicherheit erfolgen und nicht auf Grundlage des Preises und der Leistungsbeschreibung. Bei dieser Betrachtung sind kostenfreie Anbieter grundsätzlich nicht ausgeschlossen, allerdings sollte bei derartigen Angeboten stets eine kritische Prüfung der Serverstandorte und der Sicherheitsmaßnahmen des Anbieters erfolgen. Spezielle Zertifizierungen können bei der Wahl helfen, einen geeigneten Anbieter mit einem entsprechenden Sicherheitsniveau zu finden. Allerdings sind Zertifizierungen genau zu prüfen und zu hinterfragen. Nicht in allen Fällen sorgt eine vorhandene Zertifizierung auch für den gewünschten Standard.

Tipp:
Informieren Sie sich vor der Auswahl eines Anbieters über die Cloud, deren Funktionsprinzip und Sicherheitsaspekte. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat einen Katalog über Mindestanforderungen für Cloud-Anbieter formuliert.

2. Handhabung von Passwörtern

Die Lage

Mit der Zunahme an digitalen und onlinebasierten Anwendungen steigt auch die Anzahl der nötigen Accounts für die unterschiedlichen Anbieter und Dienstleister. Mit dieser Zunahme geht auch die Flut an benötigten Passwörtern einher. Passwörter sind ein bedeutender Baustein in einem Sicherheitskonzept, werden jedoch leider in zunehmenden Maße als lästiger Aufwand angesehen. Aus dieser Haltung heraus resultieren Kombinationen wie „123456“ (Platz 1*), „hallo“ (Platz 6*) oder „passwort“ (Platz 7*). Nicht gerade sichere Kombinationen, die den Zugang zu wertvollen und schützenswerten Daten sichern. Meist fehlt den Beteiligten, Inhabern wie auch den Beschäftigten, die Einsicht und Sensibilisierung im Umgang mit Passwörtern.

* Untersuchung zu den „Top Ten der deutschen Passwörter“ aus 2017 nach dem Hasso Plattner Institut.

Der Ansatz

Passwörter sind ein wichtiges Element in einem Schutzkonzept und daher auch mit der notwendigen Sensibilität zu handhaben. Unternehmen sind gut beraten in einem Sicherheitskonzept auch eine Passwortrichtlinie aufzunehmen. Wichtige Kriterien eines guten Passwortes sind bspw.:

- Passwortlänge
- Verwendete Zeichen
- Keine Wörter oder Wortkombinationen
- Einmalige Vergabe
- Regelmäßiger Wechsel

Neben den formalen Anforderungen an ein Passwort spielt auch die Handhabung eine Rolle. Passwörter sollten nicht in schriftlicher Form offen einsehbar sein oder Dritten zugänglich gemacht werden.

3. Das Sicherheitskonzept

Die Lage

Die Sicherheit der personenbezogenen Daten hat in einem Datenschutzmanagement oberste Priorität. Gerade digitale Anwendungen können Risiken für die Rechte und Freiheiten der Betroffenen bergen und sollten daher im Fokus von Sicherheitsprüfungen stehen. Nachdem detaillierte Prüfungen oftmals zeitintensiv sind und nicht zuletzt ein strukturierter Prozess für die Prüfung fehlt, werden neue Anwendungen und Applikationen kaum oder gar nicht auf Sicherheitsaspekte und Datenschutzgrundsätze geprüft und bewertet. Meist stehen der praktische Nutzen und die Effizienzsteigerung der geplanten Anwendung im Vordergrund.

Der Ansatz

Um dauerhaft die Qualität der Sicherheit gewährleisten und aufrecht erhalten zu können, ist ein Sicherheitskonzept das Mittel der Wahl. Dabei muss es sich nicht zwangsläufig um eine ausgearbeitete schriftliche Verfahrensanweisung handeln. Auch eine vollständig chronologische Auflistung der Prüfschwerpunkte für neue Anwendungen kann ausreichen. Von Bedeutung ist die zuverlässige und umfassende Prüfung und Bewertung vor der eigentlichen Inbetriebnahme.

4. Daten im privaten Umfeld

Die Lage

Kontaktdaten von Kunden oder Dienstleistern im privaten Smartphone oder die Weiterleitung einer E-Mail an die private Adresse zur Bearbeitung außerhalb der Bürozeiten. In der modernen Arbeitswelt durchaus keine Seltenheit mehr und in manchen Bereichen bereits alltäglicher oder sogar geforderter Standard. Was durchaus als besonderes Engagement gewertet werden kann, ist aus datenschutzrechtlicher Sicht eine problematische Angelegenheit. Werden personenbezogene Daten in das private Umfeld der Beschäftigten übermittelt, verliert die verantwortliche Stelle (Unternehmen) den Überblick und die Datenhoheit. Löschanträge Betroffener können nur noch bedingt erfüllt werden, da aus juristischen Gründen der Zugriff auf private Geräte der Beschäftigten nicht so ohne weiteres möglich ist und die Speicherorte zudem nicht umfassend bekannt sind. Auskunftsanfragen werden unter Umständen unzureichend beantwortet, nachdem die Empfänger oder Kategorien an Empfänger der Daten nicht oder nicht vollständig bekannt sind.

Der Ansatz

Die verantwortliche Stelle (Unternehmen) ist alleinig für die Sicherheit der personenbezogenen Daten verantwortlich. Ihr obliegt es, wirksame Maßnahmen zu ergreifen um die gesetzlichen Anforderungen zu erfüllen bzw. erfüllen zu können. Das Engagement der Beschäftigten oder der Anspruch der Kunden haben keine mildernde Wirkung auf diese Verpflichtung.
Die Vermischung von privater und geschäftlicher Korrespondenz ist bereits seit geraumer Zeit intensiver Diskussionsstoff im Datenschutzbereich. Die private Nutzung der IT-Infrastruktur der verantwortlichen Stelle (Unternehmen) ist dabei noch leichter handzuhaben als die gewerbliche Nutzung der privaten IT-Infrastruktur der Beschäftigten. Um die Vorgaben des Datenschutzes ganzheitlich erfüllen zu können, ist die Übermittlung personenbezogener Daten in das private Umfeld der Beschäftigten auf geeignete Weise auszuschließen.

5. Verdeckte Datenübermittlung

Die Lage

Bestehende Datenübermittlungen von personenbezogenen Daten an außenstehende Dritte haben in einer Datenschutzorganisation an zahlreichen Stellen Einfluss auf die zu ergreifenden Maßnahmen. Dabei ist es entscheidend, die tatsächlichen Datenübermittlungen zu kennen. In der Praxis zeigt sich häufig ein zu sorgloser Umgang mit diesem Thema. Eine Datenübermittlung erfolgt nicht zwangsläufig erst durch eine aktive Handlung der verantwortlichen Stelle (Unternehmen). Dies kann bereits passiv geschehen. Werden beispielsweise Drittinhalte in die Website eingebaut, können hierdurch bereits umfassende Daten der Besucher an den Anbieter abfließen. Spezielle Kommunikationsapps für Smartphones greifen beispielsweise das vorhandene Adressbuch ab und übermitteln die Daten in den eigenen Speicher. Übermittlungsvorgänge, die kaum beachtet werden und wofür zumeist die rechtliche Grundlage fehlt.

Der Ansatz

Jede Applikation oder jeder Inhalt, der nicht aus dem eigenen Hause stammt, ist ein potenzielles Datenschutzrisiko. Keine Technologien und Applikationen zu nutzen ist denkbar einfach und der zuverlässige Weg, aber auch gänzlich realitätsfremd. Unternehmen geraten hierdurch in eine Zwangslage. Auf der einen Seite steht die Erwartungshaltung der Kundschaft, die die digitalen und modernen Technologien voraussetzen, auf der anderen Seite sind die datenschutzrechtlichen Aspekte zu berücksichtigen. Oftmals geben bereits die AGBs (in der digitalen Zeit meist auf Englisch) der Anbieter bzw. der einzelnen Dienste Aufschluss über die Art der Daten und deren Umgang. Unklarheiten über die Handhabung der Daten sollten auf jeden Fall vorab geklärt werden. Zudem ist die Konfigurierbarkeit und die Einstellungsmöglichkeiten der Anwendung selbst zu prüfen und zu testen. Im Bedarfsfall benötigt die verantwortliche Stelle (Unternehmen) von jedem Betroffenen eine explizite Einwilligung in die vorliegende Datenverarbeitung.

Datenschutz ist die wahre Herausforderung der digitalen Epoche.